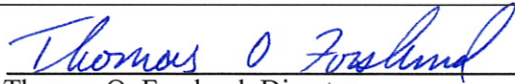
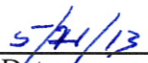


Thomas O. Forslund, Director

Governor Matthew H. Mead

Policy Title:	Physical Security
Policy Number:	S-010
Effective Date:	July 1, 2013
Approval:	<div><div> Thomas O. Forslund, Director</div><div> Date</div></div>

Purpose:

This policy establishes the minimum level of physical security required for all Wyoming Department of Health (WDH) divisions/programs/facilities.

Scope:

This policy applies to all WDH workforce.

Definitions:

Core network facilities means the cabling, equipment, and network/telecommunications rooms associated with networks that carry traffic for all buildings and external network connections on behalf of WDH.

Facility means the physical premises and the interior and exterior of a building(s).

Mobile storage device means any easily removable device that stores WDH data, including, but not limited to, laptop computers, mobile phones, external hard drives, and USB flash drives.

User means a person or entity with authorized access.

WDH Data means any data related to WDH functions that is a) stored on an information technology system, and b) maintained by WDH workforce. This applies to data in any format or media (e.g., paper, electronic, other).

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Workstation means an electronic computing device, for example a lap or desk computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

Policy:

1. General

The WDH shall implement physical security measures commensurate with identified risks.

2. Roles and Responsibilities

Responsibility for the physical security of information and technology resources shall be shared among WDH workforce who use the resources, WDH divisions/programs/facilities that house the resources, and system administrators who manage the resources.

3. Implementation of Physical Security Measures

- a. Network wiring and equipment. Network wiring and equipment rooms and cabinets shall be locked when unattended. Access shall be limited to authorized personnel and escorted visitors. Cabling and devices shall be physically secured where feasible. Core network facilities shall contain recording devices to maintain date and time of entry.
- b. Office areas. All WDH work areas shall remain locked during non-business hours (normal business hours are from 8:00 a.m. to 5:00 p.m., Mountain Standard Time, Monday through Friday, excluding holidays or emergencies) or when work areas are unattended for prolonged periods of time.
- c. Removable storage/mobile computing devices.
 - i. To safeguard and protect confidential data and information technology assets, the use of removable storage devices (e.g., USB flash drives) shall be restricted to authorized users. The user's supervisor shall authorize such use in writing. The intended use of the device shall be documented in the written authorization. Such authorization(s) shall be maintained according to division/program/facility procedures and shall minimally include:
 - A. The identification of the authorized user;
 - B. Identification of job function(s) requiring the use of a removable storage device;
 - C. The type of device utilized; and
 - D. Signatures of both the authorized user and the user's supervisor.
 - ii. Laptop computers shall be issued only to authorized division/program/facility users who shall be responsible for both the physical security of the computer and the information stored therein. All laptops shall be inventoried with a state property identification tag, shall be password protected, and shall have an appropriate level of encryption.
 - iii. Any use of personal digital assistants (PDAs) and other mobile computing devices shall meet industry security standards and shall be authorized by the user's supervisor. The use of PDAs or smart phones, etc., to access and log WDH clients' personally-identifiable information is restricted. Documentation of authorization shall be retained by the user's supervisor. The user is responsible for requesting authorization from the supervisor and notifying the supervisor of any changes relating to the use or type of equipment. Wireless access to the state network and its related equipment and components shall meet established WDH and state standards and policies.
 - iv. Mobile storage devices shall be stored securely when unattended. Storage methods include, but are not limited to:
 - A. Locking security cables that are attached directly to the device.
 - B. Storing the device in a locked cabinet or closet.
 - C. Storing the device in a locked private office.
 - D. Using reasonable security precautions when traveling (e.g., refraining from leaving a laptop unattended in a public area or hotel room).
 - v. WDH shall enable tracking and recovery software on mobile storage devices with such capabilities.
- d. Environmental security. Electrical power for servers hosting WDH services shall be protected by uninterruptible power supplies (UPS) to ensure continuity of services during power

outages and to protect equipment from damage due to power irregularities. Each UPS shall have sufficient capacity to provide at least ten (10) minutes of uptime to the systems connected to it. Systems hosting confidential data shall also be protected with a standby power generator where feasible.

- e. Visitor control. WDH shall implement visitor control procedures commensurate with identified risk to WDH data and public and client safety. Visitor control procedures may include any or all of the following:
 - i. Visitor log;
 - ii. Sign-in/sign-out records;
 - iii. Temporary badge with tracking number properly displayed; and/or
 - iv. Visitor escorts.
- f. Video monitoring. As necessary and appropriate, video monitoring shall be implemented and maintained in WDH facilities to ensure patient safety and prevent property loss. Video monitoring shall be limited to high risk areas unless otherwise necessary (e.g., JCAHO accredited facilities).
- g. Work area security. WDH work areas shall be secured to protect both sensitive and critical information and to ensure privacy. Workstations shall be strategically placed to protect the confidentiality of data. Documents and media shall be stored in a secure manner.
- h. Physical security of telecommunications resources. Telecommunication lines and equipment shall be protected to ensure both availability and confidentiality. Sensitive information shall only be sent over secure lines.
- i. Physical and environmental security for off-site storage facilities. Off-site storage facilities that store WDH information or technology shall be afforded the same level of protection as the main processing site. Adequate physical security and environmental controls shall also be implemented.
- j. Physical inventory control. The WDH fiscal division shall maintain a formal inventory of information technology assets (i.e., hardware, software, and applications) for WDH divisions/programs/facilities. Each WDH direct care facility shall maintain a formal inventory of information technology. Asset inventories shall be performed at regularly scheduled intervals or when a significant change has occurred.
- k. Controls for environmental exposures in the workplace. WDH shall protect both personnel and assets from environmental hazards by ensuring gauges, such as temperature and humidity controls, smoke detectors, and fire suppression systems, are installed and tested.
- l. Property control. Any movement of information, software media, hardware, or other physical assets shall be strictly controlled. Only authorized personnel shall be permitted to remove WDH property from WDH premises, and such personnel shall be responsible for protecting the property and controlling its use.
- m. Safety and emergency procedures. WDH regards workforce and facility safety as a high priority and shall take the steps necessary to ensure a safe workplace.
 - i. The WDH shall develop procedures for handling a variety of threats. Emergency procedures shall be written, maintained, and tested periodically at each facility for each significant threat.
 - ii. All WDH facilities shall maintain emergency equipment, as appropriate and necessary (e.g., emergency lighting, fire extinguishers) to ensure an adequate level of safety for those working within a facility. Such equipment shall be inspected annually to ensure proper operation.
- n. Incident management. Incidents shall be managed and reported consistent with WDH policies (e.g., AS-009 and S-006a; Report and Response to Privacy Violations and Security Incidents).

- o. Disposal of sensitive documents, media, and equipment. Sensitive WDH documents, media, and equipment shall be disposed of in a manner that protects the confidentiality of the information contained therein. The WDH shall develop agency-wide procedures for:
 - i. Disposal of sensitive documents.
 - ii. Destruction of computer equipment that may contain sensitive information.
 - iii. Sanitization (i.e., re-use) of equipment that might be sold or transferred to other organizations.
 - iv. Destruction of various types of media.
- p. Physical site inspections. A physical security inspection shall be performed periodically by the WDH Compliance Office or designee to ensure policy compliance. The inspection process shall be coordinated by the WDH Compliance Office. The WDH Compliance Office or designee shall notify the WDH division/program/facility of the results of physical security inspections for the purpose of remediation of deficiencies.

Contacts:

De Anna Greene, CIPP/US, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer, (307) 777-8664
Tate Nuckols, JD, WDH Security Officer, (307) 777-2438

Policies:

AS-009 and S-006a; Report and Response to Privacy Violations and Security Incidents

References:

45 CFR § 160.103
45 CFR § 164.304
45 CFR § 164.310
NIST SP-800-53

Training: